Notice of Allowability	Application No.	Applicant(s)	
	09/862,851	HOEFELMEYER ET AL.	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *10/14/2005*.

2. ☒ The allowed claim(s) is/are *1-32*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Primary Examiner
AU 2131
1/16/06

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Phouphanomketh Ditthavong on 1/12/2006.

Amend claims 1-2, 4-6, 8-10, 12-13, 16-19, 22, 24-25, 27, 30-32 as below.

1. A system for malicious code detection, comprising:

a plurality of scanning computer systems configured for scanning content for malicious code and generating an alarm when the content contains malicious code; and

a front-end processor, coupled to the plurality of scanning computer systems, configured for receiving a flow of content from an external network and distributing a common copy of the flow to each of the plurality of scanning computer systems in parallel for scanning; and

a detection management system, coupled to the plurality of scanning computer systems, configured for employing a countermeasure on the flow if at least one of the plurality of scanning computer systems generates the alarm.

2. The system according to claim 1, further comprising a database containing rules configured for creating a signature of a piece of malicious code detected by at least one of the plurality of scanning computer systems.

4. The system according to claim 3, wherein the detection management system is further configured for causing the signatures stored at the remote site detection system to be

updated to include the signature of the piece of malicious code detected by said at least one of the plurality of scanning computer systems.

5. The system according to claim 1, wherein each of the plurality of scanning computer systems is configured to execute respective anti-virus scanning software having different, corresponding coverage of malicious code.

6. The system according to claim 1, wherein the flow includes at least one of a hypertext markup file and a transferred file.

8. A system for malicious code detection, comprising: a remote site detection system configured for detecting malicious code in incoming network traffic based on signatures of malicious code stored thereat;

a plurality of scanning computer systems configured to execute respective anti-virus scanning software having different, corresponding coverage of malicious code for scanning content for malicious code and generating an alarm when the content contains malicious code; and

a front-end processor, coupled to the plurality of scanning computer systems, configured for receiving a flow of content from an external network and distributing a common copy of the flow to each of the plurality of scanning computer systems in parallel for scanning, said flow including at least one of a hypertext markup file and a transferred file; and

a detection management system, coupled to the plurality of scanning computer systems, configured creating a signature of a piece of malicious code detected by at least one of the plurality of scanning computer systems detected in the flow when at least one of the plurality of scanning computer systems generates an alarm on the piece of malicious code;

employing a countermeasure on the flow if at least one of the plurality of scanning computer systems generates an alarm on the piece of malicious code, said countermeasure including at least one of blocking the flow, quarantining the flow, and informing the recipient of the flow of the malicious code; and

causing the signatures stored at the remote site detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the plurality of scanning computer systems.

9. A method for malicious code detection in a system including a plurality of scanning computer systems, comprising:

receiving a flow of content from an external network;

distributing a common copy of the flow to each of the plurality of scanning computer systems in parallel;

scanning the flow for malicious code and generating an alarm when the content contains malicious code at each of the plurality of scanning computer systems; and

employing a countermeasure on the flow if at least one of the plurality of scanning computer systems generates the alarm.

10. The method according to claim 9, further comprising creating a signature of a piece of malicious code detected by at least one of the plurality of scanning computer systems.

12. The method according to claim 11, further comprising updating the signatures stored at the remote site detection system to include the signature of the piece of malicious code detected by said at least one of the plurality of scanning computer systems.

13. The method according to claim 9, wherein said scanning at each of the plurality of scanning computer systems includes executing respective anti-virus scanning software having different, corresponding coverage of malicious code.

16. A method for malicious code detection in a system including a remote site detection system and a plurality of scanning computer systems, comprising:

receiving a flow of content from an external network, said flow including at least one of a hypertext markup file and a transferred file;

distributing a common copy of the flow to each of the plurality of scanning computer systems in parallel;

at each of the plurality of scanning computer systems, executing respective anti-virus scanning software having different, corresponding coverage of malicious code to scan the flow for malicious code scanning and generating an alarm when the flow contains malicious code;

creating a signature of a piece of malicious code detected by at least one of the plurality of scanning computer systems detected in the flow when at least one of the plurality of scanning computer systems generates an alarm on the piece of malicious code;

causing signatures stored at the remote site detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the plurality of scanning computer systems;

employing a countermeasure on the flow if at least one of the plurality of scanning computer systems generates an alarm on the piece of malicious code, including at least one of blocking the flow, quarantining the flow, and informing the recipient of the flow of the malicious code; and

detecting malicious code in incoming network traffic based on the signatures of malicious code stored thereat.

17. A front-end system, coupled to an external network and a plurality of scanning computer systems, said front-end system comprising one or more processors, a communications interface, and a computer-readable medium bearing instructions for causing the one or more processors upon execution thereof to perform the steps of:

receiving a flow of content from the external network, said flow including at least one of a hypertext markup file and a transferred file;

duplicating the flow to produce a plurality of common copies of the flow; and distributing the common copies of the flow to each of the plurality of scanning computer systems in parallel, for scanning content for malicious code detection and alarm generation.

18. A method for operating a front-end system, coupled to an external network and a plurality of scanning computer systems, said method comprising:

receiving a flow of content from the external network, said flow including at least one of a hypertext markup file and a transferred file;

duplicating the flow to produce a plurality of common copies of the flow; and distributing the common copies of the flow to each of the plurality of scanning computer systems in parallel, for scanning content for malicious code detection and alarm generation.

19. A computer-readable medium bearing instructions for operating a front-end system, coupled to an external network and a plurality of scanning computer systems, said instructions arranged, when executed, for causing one or more processors to perform the steps of:

receiving a flow of content from the external network, said flow including at least one of a hypertext markup file and a transferred file;

duplicating the flow to produce a plurality of common copies of the flow; and

distributing the common copies of the flow to each of the plurality of scanning computer systems in parallel, for scanning content for malicious code detection and alarm generation.

22. A detection management system, coupled to a plurality of scanning computer systems, said detection management system comprising one or more processors, a communications interface, and a computer-readable medium bearing instructions arranged for causing the one or more processors upon execution thereof to perform the steps of:

receiving an alarm from one of the plurality of scanning computer systems when a common flow of content scanned by the plurality of scanning computer systems in parallel contains malicious code, said common flow including at least one of a hypertext markup file and a transferred file; and

employing a countermeasure on the common flow if at least one of the plurality of scanning computer systems generates an alarm on a piece of the malicious code.

24. The detection management system according to claim 22, wherein the detection management system is further coupled to a remote site detection system and said instructions are further arranged for causing the one or more processors to perform the steps of:

creating a signature of a piece of malicious code detected by at least one of the plurality of scanning computer systems in the flow when at least one of the plurality of scanning computer systems generates an alarm on the piece of malicious code; and

causing signatures stored at the remote site detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the plurality of scanning computer systems.

25. A method of managing malicious code detection, comprising:

receiving an alarm from one of a plurality of scanning computer systems when a common flow of content scanned by the plurality of scanning computer systems in parallel contains malicious code, said common flow including at least one of a hypertext markup file and a transferred file; and

employing a countermeasure on the common flow if at least one of the plurality of scanning computer systems generates an alarm on a piece of the malicious code.

27. The method according to claim 25, further comprising:

creating a signature of a piece of malicious code detected by at least one of the plurality of scanning computer systems in the common flow when at least one of the plurality of scanning computer systems generates an alarm on the piece of malicious code; and

causing signatures stored at a remote site detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the plurality of scanning computer systems.

28. A computer-readable medium bearing instructions for managing malicious code detection, said instructions arranged for causing the one or more processors upon execution thereof to perform the steps of:

receiving an alarm from one of a plurality of scanning computer systems when a common flow of content scanned by the plurality of scanning computer systems in parallel contains

malicious code, said common flow including at least one of a hypertext markup file and a transferred file; and

employing a countermeasure on the common flow if at least one of the plurality of scanning computer systems generates an alarm on a piece of the malicious code.

30. The computer-readable medium according to claim 28, wherein said instructions are further arranged for causing the one or more processors to perform the steps of:

creating a signature of a piece of malicious code detected by at least one of the plurality of scanning computer systems in the common flow when at least one of the plurality of scanning computer systems generates an alarm on the piece of malicious code; and

causing signatures stored at a remote site detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the plurality of scanning computer systems.

31. The system according to claim 1, wherein each one of the plurality of scanning computer systems is configured to execute malicious code detection software other than detection software executed by any other one of the plurality of scanning computer systems.

32. The method according to claim 9, wherein said scanning at each of the plurality of scanning computer systems includes executing malicious code detection software other than detection software executed by any other one of the plurality of scanning computer systems.

Examiner's Statement of Reasons for Allowance

Claims 1-32 are allowed over prior art of record.

The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.

None of the prior art of record, either taken by itself or in any combination, would have anticipated or made obvious the invention of the present application at or before the time it was filed. The subject matter regarded as allowable by the examiner is found in claims 1, 8, 9, 16-22, 25, 28 , where common copy of the flow (i.e. the same flow) is duplicated and distributed in parallel to a plurality of scanning computer systems configured for scanning content for malicious code.

Dependent claims 2-7, 10-15, 23-24, 27, 29-32 are also allowed over prior art of record by virtue of their dependencies.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Prior arts made of record, not relied upon:

Pub. No. US 2003/0191957 to Hyponen et al. is directed to a method of detecting viruses in a computer network comprising intercepting data at least one data transit node of the network . The transit node identifies which of the data is of a type capable of containing a virus and transfers the identified data to a virus scanning server over the network . The identified data is received at the virus scanning server which scans the data to identify viruses present therein. The server subsequently acts in dependence upon the outcome of the virus scan.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T.A.

Taghi T. Arani, Ph.D.
Examiner
Art Unit 2131
1/12/2006

Primary Examiner
AU 2131
1/16/06